REMARKS

1. SUMMARY OF THE OFFICE ACTION

Claim 37 stands rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. Claims 1-13, 19-24, 26-43, and 50-78 stand rejected under the judicially created doctrine of double patenting in view of U.S. Patent No. 6,658,567. Claims 1, 4 7-9, 11-13, 19-24, 26-28, 31-35, 40-43, 50-51, 53-66, 69, 72-74, 76-78 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 5,991,399 to Graunke et al. (hereinafter, "Graunke"). Claims 2-3, 29-30, 52, and 67-68 stand rejected under 35 U.S.C. 103(a) as being obvious in light of the combination of Graunke and U.S. Patent No. 6,687,375 to Matyas, Jr. et al. (hereinafter, "Matyas").

2. RESPONSE TO § 112, FIRST PARAGRAPH REJECTION

The Examiner has rejected claim 37 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. In particular the Examiner has stated:

> Examiner was unable to find the teachings regarding "sending the locked specific copy of the application program and specific conduit data from the user to the software supplier."

(Office Action mailed 3-18-2004).

To satisfy the written description requirement, a patent specification must describe the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention. See, e.g., Vas-Cath, Inc. v. Mahurkar, 935 F.2d at 1563, 19 USPQ2d at 1116. Whenever the issue arises, the fundamental factual inquiry is whether the specification conveys with reasonable clarity to those skilled in the art that, as of the filing date sought, applicant was in possession of the invention as now claimed. Vas-Cath, Inc. v. Mahurkar.

Applicants submit that the following excerpt from the specification provides sufficient support to overcome the Examiner's rejection:

> Referring first to **Figure 4A**, conduit data 98 may be provided by a conduit inspection service company 96 such as, for example, BlackHawk Pipeline Assessment Services of Atlanta, Georgia, to the

> end user 100. Conduit data 98 may be stored on a compact disk (CD) 99. The end user 100 then provides the conduit data 98 on the CD 99 to the analyzer software supplier 102.

(Applicant's Specification, Paragraph beginning at line 20 of page 13, emphasis added). Applicants are aware that the cited paragraph does not specifically refer to "sending the ... application program ... from the user to the software supplier." However, the subject matter of the claim need not be described literally (i.e., using the same terms) in order for the disclosure to satisfy the description requirement. Furthermore, the claim language itself may describe the invention even if no corresponding description is in the disclosure. Therefore, Applicants submit that the specific claim language cited by the Examiner, when read in light of the above referenced paragraph from the specification, conveys with sufficient clarity to one skilled in the art that Applicants were in possession of the claimed invention at the time the application was filed.

3. RESPONSE TO NON-STATUTORY DOUBLE PATENTING REJECTION

The Examiner has rejected claims 1-13, 19-24, 26-43, and 50-78 under the judicially created doctrine of obviousness-type double patenting over claims 1-49 of U.S. Patent no. 6,658,567.

Applicants respectfully traverse the double patenting rejection. However, for the purpose of economy of prosecution, included is a terminal disclaimer to overcome the double patenting rejection.

4. RESPONSE TO § 102 REJECTIONS

Applicants respectfully traverse this rejection for the reasons set out below, and ask the Examiner for reconsideration.

To anticipate a claim, the reference must teach every element of the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

- **Independent claims 1, 21 (as amended), 50, 56, 61, 64 (as amended), and 66 are not anticipated by Graunke, because Graunke does not teach each and every element of the claims, as amended.**

Claim 1, representative of the group, includes the following:

> A method of locking conduit data and an analyzer program that analyzes the conduit data, the method including:
>
> generating a first key;
>
> associating the first key with both specific conduit data and a specific copy of the analyzer program; and
>
> generating a gatekeeper logic that, utilizing at least the first key, prevents the specific copy of the analyzer program from analyzing conduit data other than the specific conduit data.

(Claim 1, emphasis added).

Graunke, on the other hand, discloses the following:

> The storage device reader 16 interacts with a key module 18, which is downloaded from a communications network or otherwise accessed by the storage device reader. The key module 18 verifies that the storage device reader is authentic and that access to the digital content is allowed. The key module uses a key integral with the key module to decrypt the encrypted digital content. If the storage device reader is verified and it is indeed the authorized storage device reader software asking the key module for access to the digital content, then the digital content is decrypted by the key module. Otherwise the digital content is not decrypted. Hence, the key module ensures that the party requesting the decryption of an encrypted digital content is authentic and its integrity is verified. Preferably, key module 18 is provided dynamically by a content provider from a remote system over a communications network such as the Internet.
>
> ...
>
> At step 102, a content provider creates digital content, encrypts the content using one or more symmetric keys, and stores the corresponding symmetric keys in the same or another secure database.
>
> ...
>
> When the user desires to play the encrypted content, he or she directs the trusted player on the client system to initiate the performance operation through a well-known graphical user interface. At step 106, the trusted player requests the symmetric keys for decrypting the encrypted content from the server by sending a copy of the trusted player's manifest and the user's information regarding the title of the content and optionally, financial information for the transaction, to the key control software within the server.

(Graunke, Col. 4, Line 45; Col. 8, Line 2; and Col. 8, Line 10, emphasis added).

In short, Graunke discloses a system that encrypts digital content with a symmetric key, and stores the symmetric key in a database. According to Graunke, the trusted player must request the symmetric key from a server in order to decrypt the content. Consequently, the trusted player referred to in Graunke is prevented from accessing content by the encryption of that content. However, if the key module sent to the player from the server successfully authenticates the trusted player, then the digital content is decrypted. Consequently, the key module does not prevent the specific copy of the analyzer program from analyzing conduit data other than the specific conduit data, as is claimed in claim 1. For example, the key module does not prevent the trusted player from accessing encrypted data. Instead, the key module authenticates the player and facilitates the decryption of symmetric keys that are used to access the data. Furthermore, Graunke does not disclose associating a first key with both specific conduit data and a specific copy of the analyzer program, as is claimed in claim 1.

In the Office Action mailed March 18, 2004, the Examiner references most of column 8, including lines 19 through 28, which state:

> Key control then generates the key module by execution of the following steps. First, key control generates an asymmetric key pair at step108. Next, at step 110, key control obtains the symmetric keys associated with the user-selected content from the database and encrypts the symmetric keys using the generated asymmetric public key. Finally, at step 112, key control builds a tamper resistant key module with the generated asymmetric public key, the now-encrypted symmetric keys, and the asymmetric public key for the manifest of the trusted player from the database.

(Graunke, Col. 8, Lines 19-28). Applicants submit that the referenced passage does not disclose associating a first key with both specific conduit data and a specific copy of an analyzer program, as is claimed in claim 1. According to Graunke, the asymmetric private key, which the Examiner suggests is analogous to the key in claim 1, is added to a key module and transmitted to a trusted player. At the trusted player, the asymmetric private key is used to decrypt symmetric keys – the symmetric keys used to decrypt content that is then played on the trusted player. However, the asymmetric private key is not associated with the player, nor is it associated with the encrypted digital content.

Therefore, for the above reasons, Graunke does not anticipate claims 1, 21 (as amended) 50, 56, 61, 64 (as amended), and 66 under 35 U.S.C. §102(e) because Graunke does not disclose each and every limitation of claims 1, 21, 50, 56, 61 and 64. Accordingly, Applicants submit

that claims 1, 21, 50, 56, 61, 64 and 66 are patentable over Graunke and in condition for allowance. Given that claims 2-18, 51-55, and 67-78 depend directly or indirectly on claims 1, 50 and 66 respectively, Applicants submit that claims 2-18 and 51-55 are not anticipated by Graunke and are also in condition for allowance.

Independent claims 19, 20, 57, 62 and 63 are not anticipated by Graunke, because Graunke does not teach each and every element of the claims.

Claim 19, representative of the group, includes the following:

> A method of executing an analyzer program to analyze conduit data to which it is locked, the method including:
>
> determining a first key associated with a specific copy of an analyzer program;
>
> determining a second key associated with specific conduit data;
>
> determining a characteristic parameter representative of a characteristic of the specific conduit data;
>
> deriving a gate key utilizing the second key and the characteristic parameter; and
>
> allowing execution of the specific copy of the analyzer program to analyze the specific conduit data if the gate key corresponds to the first key.

(Claim 19, emphasis added).

According to claim 19, a characteristic parameter representative of a characteristic of the specific conduit data is determined and a gate key is derived utilizing the characteristic parameter. For example, the specification states at line 19 of page 8:

> For example, the characteristic parameter may be the size of a conduit data file 12, and the characteristic value attributed to this parameter may be actual size of a conduit data file 12 expressed in bits, bytes or any other measure.

(Specification, Line 19, Page 8). According to claim 19, for example, the characteristic parameter (e.g., conduit data file size) may be used to derive a gate key.

Graunke, on the other hand, discloses generating a key module to transfer from a server to a trusted player in order to authenticate and verify the player. According to Graunke, the key module contains an asymmetric private key (e.g., to decrypt the symmetric keys), encrypted symmetric keys (e.g., to decrypt content), and an asymmetric public key (e.g., to authenticate the

player). However, Graunke does not disclose using a characteristic parameter representative of a characteristic of conduit data to derive a gate key, as is claimed in claim 19.

Therefore, for the above reasons, Graunke does not anticipate claims 19, 20, 57, 62 and 63 under 35 U.S.C. §102(e) because Graunke does not disclose each and every limitation of claims 19, 20, 57, 62 and 63. Accordingly, Applicants submit that claims 19, 20, 57, 62 and 63 are patentable over Graunke and in condition for allowance.

Independent claims 26 and 65 are not anticipated by Graunke, because Graunke does not teach each and every element of the claims.

Claim 26, representative of the group, includes the following:

> A method of distributing conduit data and an analyzer program that analyzes the conduit data, the method including:
>
> providing a user of the analyzer program with a specific copy of the analyzer program;
>
> providing the user of the analyzer program with a locking logic that locks the specific copy of the analyzer program to selected conduit data; and
>
> providing the user of the analyzer program with a gatekeeper logic that allows the specific copy of the analyzer program to analyze only the selected conduit data.

(Claim 26, emphasis added).

According to claim 26, locking logic that locks a specific copy of an analyzer program to selected conduit data is provided to the user. Furthermore, gatekeeper logic that allows the specific copy of the analyzer program to analyze only selected conduit data is provided to the user. For example, beginning on line 25 of page 15, the specification states:

> Figure 4C shows a further method 94 of distributing conduit data and an analyzer program, which are locked, to an end user 100. While the conduit inspection service company 96 provides the conduit data 98 to the end user 100, as in the methods 90 and 92 above, this conduit data 98 is not provided to the analyzer software supplier 102. In the method 94, the analyzer software supplier 102 provides a further package 108 to the end user 100, the package 108 including a copy-protected and read-protected copy of the analyzer application source code 26, a copy of the locking routine 14, and a purge routine 106. The end user 100 then executes the locking routine 14 to enable the analyzer application 30 locally to generate the first key 18, the gatekeeper application 24 and the second key 22. Following compilation of a specific and compiled copy of the analyzer

> application 30, and the embedding of the second key 22 within a conduit data file 12, the purge routine 106 will then automatically be invoked to purge the locking routine 14 and the analyzer application source code 26 from a computer system operated by the end user 100. The end user 100 will then retain only the package 32, the other software having been purged from a relevant computer system by the purge routine 106.

(Specification, Page 15, Line 25).

Graunke does not disclose providing the user with a locking logic that locks a specific copy of an analyzer program to selected conduit data. Therefore, for the above reasons, Graunke does not anticipate claims 26 and 65 under 35 U.S.C. §102(e) because Graunke does not disclose each and every limitation of claims 26 and 65. Accordingly, Applicants submit that claims 26 and 65 are patentable over Graunke and in condition for allowance.

Independent claim 27 is not anticipated by Graunke, because Graunke does not teach each and every element of the claims.

Claim 27, includes the following:

> A method of distributing conduit data and an application program that accesses the conduit data, the method including:
>
> locking a specific copy of the application program to specific conduit data so that the specific copy of the application program is able to access only the specific conduit data; and
>
> distributing the locked specific copy of the application program and specific conduit data to a user.

(Claim 27, emphasis added). According to claim 27, a specific copy of an application program is locked to specific conduit data so that the specific copy of the application is able to access only the specific conduit data.

Graunke, however, discloses a trusted player with a signed manifest. The trusted player is not restricted to particular content. Rather, for each particular content, the player must request a symmetric decryption key from a server. Graunke does not disclose locking a specific copy of an application program to specific conduit data so that the specific copy of the application program is able to access only the specific conduit data, as claimed in claim 27. Therefore, for the above reasons, Graunke does not anticipate claim 27 under 35 U.S.C. §102(e) because Graunke does not disclose each and every limitation of claim 27.. Accordingly, Applicants submit that claim 27 is patentable over Graunke and in condition for allowance.

5. RESPONSE TO § 103 REJECTIONS

Applicant(s) respectfully traverse this rejection for the reasons set out below, and ask the Examiner for reconsideration.

To establish a **prima facie** case of **obviousness**, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The Examiner has rejected claims 2-3, 29-30, 52, and 67-68 under 35 U.S.C. §103(a) for being obvious in light of the combination of Graunke and Matyas. Claims 2-3, 29-30, 52, and 67-68 are dependent upon independent claims 1, 27, 50 and 66 respectively. Because Matyas does not disclose the above limitations in the independent claims that Applicant submits are not disclosed by Graunke, the independent claims are not obvious in light of the combination of Graunke and Matyas. Consequently, the dependent claims cannot be obvious in light of the combination of Graunke and Matyas.

In light of the above, Applicant(s) respectfully submit(s) that the rejection under 35 U.S.C. § 103 has been overcome, and withdrawal of this rejection is therefore respectfully requested.

6. CONCLUSION

Having tendered the above remarks and amended the claims as indicated herein, Applicants respectfully submit that all rejections have been addressed and that the claims are now in a condition for allowance, which is earnestly solicited.

If there are any additional charges, please charge Deposit Account No. 02-2666. If a telephone interview would in any way expedite the prosecution of the present application, the Examiner is invited to contact Nathan Elder at (408) 947-8200 ext. 207.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 7-1-04, 2004

Nathan P. Elder
Reg. No. 55,150

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 947-8200